Introducción a la Teoría de Números
Curso 2012

Lista 3. Criptografía – entrega 28/9

1. Descifrar el siguiente criptograma:

```
idqgq sifmc irpgk sjlpm egmci riqmp iqfty emrgd
cipjf kiprj fmumq smrjh amrip thqgf kdiiq stcgj
cidme pirti hrgmc imkmp grgjh cirmc mqgfu jdjih
idrpg ksjlp mfmkt hsjih iqsir mqjrj fmkmp mqgfk
dgegr mprjf mtqmf jqqjd mfihs idisp mqfgh tqrtd
mqqgh mrihs jqkth sjiqt qtmdg lhjpm pdjqi qkmrg
jqyml ptkmp dmqdi spmqi hudjn tiqnt ijrtd smhdm
qikmp mrgjh ihkmd mupmq kthsj
```

   (sugerencia: estudiar la frecuencia de aparición de cáda letra.)

2. Walter crea una clave de RSA con un modulo n suficientemente grande de modo que no puede factorizarse en tiempo razonable., Álvaro utiliza esta clave para enviarle mensajes a Walter de la siguiente manera: representa cada carácter como un entero entre 0 y 27 ($\mathtt{A}$ representado por 1, $\mathtt{B}$ por 2, etc. y un espacio por 0), y encripta cada número individualmente usando la clave pública de Walter. ¿Es este método seguro?

3. Para $n \in \mathbb{N}$ sea $\sigma(n)$ la suma de los divisores de n; por ejemplo, $\sigma(6) = 1 + 2 + 3 + 6 = 12$ y $\sigma(10) = 1 + 2 + 5 + 10 = 18$. Supongamos que $n = pqr$ con p, q, y r primos distintos. Dar un algoritmo eficiente que, dados n, $\phi(n)$ y $\sigma(n)$, encuentre la factorización de n. Usar este algoritmo para factorizar $n = 60071026003$ sabiendo que $\phi(n) = 60024000000$ y que $\sigma(n) = 60118076016$.

4. Queremos acordar una clave secreta con José usando el sistema Diffie-Hellman. José nos anuncia que $p = 3793$ y que $g = 7$. En secreto, José elije un número $n < p$ y nos dice que $g^n \equiv 454 \pmod{p}$. Elegimos el número $m = 1208$. ¿Cuál es la clave secreta?

5. Espiamos una conversación entre Walter y Álvaro en la que acuerdan una clave secreta usando Diffie-Hellman; ellos elijen $p = 97$ y $g = 5$. Walter elije un número n y dice a Álvaro que $g^n \equiv 3 \pmod{97}$, y Álvaro elije un número m y dice a Walter que $g^m \equiv 7 \pmod{97}$. Romper el código por fuerza bruta: ¿Cuál es la clave secreta en la que se han puesto de acuerdo? ¿Cuál es n? ¿Cuál es m?

6. En este problema se trata de "romper" un criptosistema RSA. ¿Cuál es el número secreto d que sirve para decodificar el sistema RSA con clave pública

$$(n, e) = (5352381469067, 4240501142039)?$$

7. Álvaro crea una clave de RSA con clave pública

$$(n, e) = (1433811615146881, 329222149569169).$$

   (a) De alguna forma descubrimos que $d = 116439879930113$. Mostrar como usar el algoritmo probabilistico para factorizar n conociendo d.

   (b) En la parte (a) se ve que los factores p y q de n son muy próximos. Mostrar como usar el método de factorización de Fermat para factorizar n.